Fauquier County Government & Public Schools

FINANCE DEPARTMENT
320 Hospital Drive
Suite 32
Warrenton, VA 20186-3037

Telephone (540) 428-8729 *Fax (540) 341-1005*

To: Chairman and Members of the Board of Supervisors
Chairman and Members of the School Board
County Administration
Schools Administration

From: *Vivian McGettigan*, Finance Director
Rick Klinc, Information Technology Director

Subject: Corrective Action Plan: FY 2006 Management Letter

Date: *December 1, 2006*

On behalf of all those involved in the financial statement preparation for Fauquier County, we appreciate the suggestions given by the County's Independent Auditor for improvements. We have reviewed the Audit Management Letter, and present our strategies to enhance the quality of our processes. In the paragraphs below are outlined our response to the Auditor's recommendation. This comment relates to a multi-year project, therefore the progress in FY 2005 and FY 2006 has been presented.

Fiscal Year 2005

Audit Comment: **Repeat Comment - Computer Controls** – Our prior audit revealed that the County should develop a disaster recovery / contingency plan for its various operating systems. Such a plan would help recovery from data loss, hardware failure, and other potential problems more quickly in the event of a disaster. The plan should include procedures necessary for restoration of backup data. The plan will also help the County forecast potential problems and proactively plan around them rather than having to react to any situation that arise. During the current year the County has developed certain aspects of the plan, although they have not been put in writing. We recommend the County document in writing its disaster recovery / contingency plan.

Response: **2005 PARTIALLY IMPLEMENTED** - Through the Technology Review Board, the Information Technology Department has begun the process of developing a disaster recovery plan. Development and implementation of this plan will be a multi-year effort. The first step in developing a disaster recovery plan is identifying the most likely causes of failure and addressing them in priority. Creating the proper environment for information technology equipment has been identified as the most critical issue in preventing system failure and is being addressed through the County's Facilities Planning and Implementation Committee. In conjunction with preventive efforts, mission critical individual systems will need to be identified and prioritized for disaster recovery before a formal plan can be prepared. To

achieve the goal of developing a disaster recovery plan it is essential to consider both existing technology and future acquisitions. For existing technology, the cost to correct any deficiencies will need to be evaluated relative to the benefit gained. For future acquisitions, disaster recovery issues will need to be incorporated in the planning phase of any new technology systems.

In the interim period several steps have already been taken to provide backup in the event of system failures. The Information Technology Department has fully implemented the auditors' recommendation related specifically to recovery from data loss and hardware failure for mission critical systems. The next step is to form a Disaster Recovery Team to identify disaster recovery for business operations which goes beyond information technology. The disaster recovery plans should include contingency procedures in the event technology is not available potentially disrupting business operations. For example, the inability to access office files, due to the closure of a building from a structural building problem or event of nature. The final stage would be to formally document the recovery plan.

2006 PARTIALLY IMPLEMENTED – The design and approval of the data center construction process consumed most of FY2006. Construction began in June of 2006 and is scheduled to be completed by the end of January, 2007. A similar construction project is now underway at the Sheriff's Office which will improve the environment for the data equipment that is located in that facility.

As mentioned in last year's response, backup's are performed on a regular basis for mission critical data and taken to an offsite location. The combination of critical system back-ups and improving the environment completes the first part of our Disaster Recovery efforts. The next step in Disaster Recovery planning for Fauquier County would be to form a project team consisting of key business unit personnel to define their requirements for recovery. Although the IT Department needs to be involved in this process, this should not be considered an IT project.